12-1-2009

Security Issues Challenging Facebook

S Leitch
Edith Cowan University

M Warren
Edith Cowan University

DOI: 10.4225/75/57b4188730df5
7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2009

Security Issues Challenging Facebook

S.Leitch & M.Warren,
School of Information Systems,
Deakin University
Melbourne, Australia.

Abstract

The advancement in Internet and bandwidth capability has resulted in a number of new applications to be developed; many of these newer applications are described as being Web 2. A Web 2 application such as Facebook has allowed people around the world to interact together. One of the interesting aspects of Facebook is the use of third parties applications and the interactions that this allows.Not surprisingly, the problems that exist in the real world such as theft, fraud, vandalism also exist in online Web 2 environments. This paper explores and categorises several security issues within the Facebook environment. It contributes to practice and research by emphasising the importance of security awareness in the use of Web 2 applications such as Facebook.

Keywords

Facebook, Security Issues

INTRODUCTION

Information can be accessed anytime, anywhere and in any place is one the features of the twenty first century. The wide spread adoption of Electronic Business and fast internet access through broadband provides access to business and commerce to anyone at anytime. The emergence of Web 2 and related internet applications such as Facebook has had a major impact upon the Internet in recent years. One of the interesting aspects of Facebook is the use of third parties applications and the interactions that this allows. This means that individual Facebook pages now act as a web page, blog, instant message, email systems and the use of third parties applications allows for real time functionality (DiMicco and Millen, 2007; Shuen, 2008).

In terms of this paper, the research team has focussed upon considering the security issues within the Facebook applications. The reason for this is the rise in popularity of this particular application and the increasing number of security issues which have arisen.

FACEBOOK

The Information Society has developed in recent years and impacts all aspects of society. The global impact of the internet can be shown by Table 1.

Table 1 - Global Internet Usage (InternetWorld, 2009)

Region	Number (Millions of Users)	% Regional Penetration
Asia	704.2	18.5
Europe	402.4	50.1
North America	251.7	73.9
Latin America / Caribbean	175.8	30
Africa	65.9	6.7
Middle East	48	23.7
Oceania / Australia	20.8	60.1
World Average		24.7

The global impact of the Internet is shown by Figure 1; of particular interest is the impact that the Internet has upon North America, Oceania and Europe. The impact of the Internet upon Australia and New Zealand can be seen by Figure 2 and highlight how some countries can experience high usage of the Internet.

Table 2 - Australia and New Zealand Internet Usage (InternetWorld, 2009b)

Region	Number (Millions of Users)	% Country Penetration
Australia	16.92	79.6
New Zealand	3.36	79.7

The environment of increasing numbers of Internet Users and a faster internet has allowed for Web 2 to be devolved (Shuen, 2008). One of the leading Web 2 applications is Facebook.
Facebook was founded in February 2004. Facebook is a social utility that helps people communicate more efficiently with their friends, family and co-workers. The company develops technologies that facilitate the sharing of information through the social graph, the digital mapping of people's real-world social connections. Anyone can sign up for Facebook and interact with the people they know in a trusted environment (Facebook, 2009a)

Facebook has had a global impact (Facebook, 2009b):

- More than 300 million active users;
- 50% of our active users log on to Facebook in any given day;
- Average user has 130 friends on the site;
- More than 6 billion minutes are spent on Facebook each day (worldwide);
- More than 350,000 active applications currently on Facebook Platform;
- More than 250 applications have more than one million monthly active users;
- more than 65 million active users currently accessing Facebook through their mobile devices;
- Facebook employ 900 staff.

FACEBOOK SECURITY ISSUES

The researchers adopted and amended a security incident model that was used to model Virtual World Security Threat Matrix (STM) (Lee and Warren, 2007). This model was used to identify security risks associated with using Second Life, which is a graphical virtual system.

The model was amended to analyse the security threats posed by Web 2 applications such as Facebook. The research team modified the framework to cater for the specific Facebook environment.

The research team acknowledges that the modified framework may not be exhaustive in identifying all the different security dimensions. As with the Virtual STM (Lee and Warren, 2007), it is important to note also that the security dimensions are not listed according to any order of importance. The Facebook STM can be found in Figure 1:

Security Threat Dimension	***Nature of issue***	***Implication***
I. Privacy & Confidentiality	▪ Information exchanged and transmitted between third party applications and Facebook applications may not be private. Text chat, voice chat and private instant message between users may not be encrypted. ▪ Third Party applications may be used to record and online conversation between users without the expressed consent of users. ▪ Facebook users may accidently alter their privacy settings and unintentionally release their information.	▪ Organisations will need to develop guidelines and policies to determine what information may/may not be discussed in Facebook, and how stakeholders will be notified if they are being monitored. ▪ Facebook users would need to be educated about the privacy issues in relation to Facebook. ▪ Companies such as Telstra have established guidelines that restrict employees from discussing commercial-in-confidence information within Social Media Sites. ▪ Facebook would need to ensure that users are educated about the privacy issues in relation to Facebook.

II. Authentication & Identity Theft	▪ Verifying the identity of a Facebook user could be an issue. Identity theft is possible if social engineering techniques or by the use of key logging software. ▪ Some third party applications may require credit card registration for identity verification or alternative payment systems, e.g.in the Battlestations application you can purchase *ochos* using your credit card and spend *ochos* during the game.	▪ Difficulty in verifying identify due to limited Facebook authentication, e.g. user name and password and Facebook request a mobile phone number in certain circumstance, e.g. being able to quickly reply to messages. ▪ Difficulties in ensuring security since applications are third party. Educate Facebook users about using secure socket layer (SSL) applications.
III. Intellectual Property Theft	▪ Theft of Intellectual Property in (a) Existing copyrighted materials, e.g. video, music.	▪ Difficulties in ensuring that video and audio content streamed in Facebook do not breach existing copyright laws.
IV. Vandalism, Harassment & Stalking	▪ Stalking of friends and harassment is a potential issue.	▪ Facebook users can exclude and block potential friends. Any incident can be reported to Facebook for further investigations.
V. Defamation & Disparagement	▪ Deception, spreading false and misleading information rumour mongering. ▪ Libel, defamation and slandering ▪ Disparagement remarks real world products.	▪ Dealing with negative comments, is something that an individual user can resolve, e.g. delete comment or remove friend. If the situation is serious then the matter can be reported to Facebook. There is a developing trend of media reporting Facebook entries. ▪ Balancing freedom of speech and censorship in Facebook. ▪ Ensuring that culturally sensitive issues and actions that affect the stability of societies are addressed in Facebook.
VI. Spam & Cybersquatting	▪ Unsolicited emails and messages that may contain viruses or malware.	▪ A major dilemma for Facebook is the growth of spam. The potential risks relate to identify theft and the issues associated with third party software.
VII. Payment and	▪ As mentioned before,	▪ Difficulties in ensuring

Transaction Integrity	some third party applications may require credit card registration for identity verification or alternative payment systems, e.g.in the Battlestations application you can purchase *ochos* using your credit card and spend *ochos* during the game.	security since applications are third party. Educate Facebook users about using secure socket layer (SSL) applications.
VIII. Malwares and Computer Virus	▪ Unsolicited emails and messages that may contain viruses or malware.	▪ Educating Facebook users about the potential threat associated with malware and viruses being sent via Facebook, e.g. having an updated virus and spyware checker.

Figure 1 - Facebook STM (Based upon Virtual World STM (Lee and Warren, 2007)

FACEBOOK SECURITY BREACH EXAMPLES

The following are examples of Facebook security breaches:

Identify Theft

New laws introduced by the Attorney General of Australia introduced jail terms of up to ten years for individuals using networking sites such as Face book to steal identities without having to wait for them to obtain money as a part of the fraud (Hildebrand, 2009). This stance by the Australian Government clearly indicates the severity and rampant nature of identity theft on social networking sites. The premise of these sites is the sharing of personal information with a group of "friends", unfortunately as sites such as Facebook have expanded many users now have friends that are not known to them in person. This change in the nature of the use of Facebook has meant that for those criminals seeking personal information in order for financial gain, it has become much easier. Many users of Facebook under utilise the privacy and security options available to them, and simply fail to consider the importance of the information they are sharing (Strater and Richter, 2007).

Viral wall messages, phishing, malware spam advertising by third party applications have all been linked to security and privacy breaches involving social networking sites. Identity theft worms are common and have been spreading throughout Facebook enticing users, for example, to click links commenting, "find out what other users are saying about you" which spreads the worm through the Facebook messaging capabilities (Dimmel, 2008).

Third Party Applications

In late September, 2009 an online Facebook poll entitled, "Should Obama be killed?" posted. The US secret service was called upon to investigate this possible threat and to trace the creator of the poll. Whilst it proved to be a childish prank it has surfaced another range of issues related to the privacy and security aspects of social networking sites, such as (Ostrow, 2009):

- Should social networking sites take more care and responsibility in policing themselves and the content posted by their members?;
- Is there a limit to the expression of personal opinions and when do those opinions breach security and privacy standards;
- Do government and law enforcement have a role? (this has resurfaced in new way since the rise of social networking).

The online poll was posted through a third party application and therefore not directly controlled by Facebook, which raises a key question about the control that Facebook has over it its own application. Facebook uses many third party applications, this is going to make social networking much more difficult to control and "police".

Organisational impact

With the large number of Internet users now delving into the world of social networking, the time and usage of such software has become a concern in regards to the impact it may have on organisations. While much emphasis is placed on the "lost working hours" of employees use of Facebook and other software, it should also be considered that social networking software can also have a positive benefit on an organisation through the use of inter and intra organisational social networking.

Negative impacts can be loss of productivity, affected system resources, financial costs, organisational power issues (refusal of a worker to make the boss a "friend"), confidentiality of individuals and that Facebook should be used for non-commercial purposes however positively it can build strong intra organisational links, provide a human face to an organisation or quite simply give employees a break from their everyday work. The decision of blocking social networking sites has become contentious for these and other issues, with one report of anecdotal research indicating that 46% of potential employees (with two job offers) would choose the employer who does not block its use (Abrahams, 2008).

It is becoming more popular within large organisations for there to be an acceptable usage policy for employees' use of social networking sites, this has been driven by some of the problems mentioned above and it's being mandated by management of an organisation and formulated by Human Resources departments.

The personal security and individuals should be seriously considered when assessing organisational use, including the trawling of sites for information of potential employees (political persuasions, sexual orientation etc) or even health insurance providers attempting to glean information to further their own organisational goals (refusal to cover based on obtained information).

CONCLUSION

This paper has assessed a number of real life security issues and threats associated with facebook. The outcome of the research is that the same security risks and threats that exist within the general internet community also relate to facebook. In many cases these risks are greater for systems such as Facebook, e.g. the fact that people trust their Facebook friends means that the potential impact for identify theft is even greater.

This paper contributes to practice and research by providing a broad overview of security issues faced when using Facebook. The next stage of the research is to analyse a number of different security incidents that relate to Facebook.

REFERENCES

Abrahams, N. (2008). The pain and potential of Facebook in the office, Sydney Morning Herald. http://www.smh.com.au/technology/biz-tech/the-pain-and-potential-of-facebook-in-the-office-20090616-ce7d.html, Accessed 18th Oct 2008.

Dimmel, B. (2008). Identity theft worm hits Facebook. http://www.infopackets.com/news/security/2008/20081208_identity_theft_worm_hits_facebook.htm. Accessed 18th Oct 2009.

DiMicco, J. M. and Millen, D. R. (2007). Identity management: Multiple presentations of self in Facebook. Proceedings of the ACM Conference on Organizational Computing and Groupware Technologies (GROUP 2007).

Facebook (2009a) Facebook Facts, URL: http://www.facebook.com/press/info.php?factsheet, Accessed 25th September, 2009.

Facebook (2009b) Facebook Statistics, URL: http://www.facebook.com/press/info.php?statistics, Accessed 25th September, 2009.

Hildebrand, J. (2009). Facebook identity Theft enough for jail. http://www.news.com.au/story/0,27574,25764253-421,00.html. Accessed 20th July 2009.

InternetWorld (2009a) Global Internet Statistics, URL: http://www.internetworldstats.com/stats.htm, Accessed 25th September, 2009.

InternetWorld (2009b) Australian and New Zealand Internet Statistics, URL: http://www.internetworldstats.com/stats.htm, Accessed 25th September, 2009.

Lee, C. and Warren, M. (2007) Security Issues within Virtual Worlds such as Second Life, Proceedings of the 5th Australian Information Security Management Conference, Edith Cowan University, Western Australia.

Ostrow, A. (2009). Obama Assassination poll on Facebook was created by a minor. http://mashable.com/2009/10/01/kill-obama-poll. Accessed 1st October 2009.

Shuen, A. (2008). Web 2.0: a strategy guide. O'Reilly Media, Inc.

Strater, K. and Richter, H. (2007). Examining privacy and disclosure in a social networking community. In SOUPS '07: Proceedings of the 3rd ACM symposium on Usable privacy and security, New York, NY, USA, 2007 (pp. 157-158).

COPYRIGHT